REMARKS

Claims 1-25 are pending in the present application. The Applicants respond to the issues identified in the Office Action mailed on November 17, 2006 as follows:

Drawings

Figure 1 has been corrected so that "ISP Date Center..." now reads "ISP Data Center..." A replacement drawing sheet for FIG. 1 is attached.

Claim Objections

Claim 25 has been amended so that it now depends on claim 16 in accordance with the Examiner's suggestion.

Claim Rejections -- 35 USC § 102

Claims 1-4 and 14 have been rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Publication No. US 2003/0103615 to Baltes ("Baltes"), which discloses a method for automatically configuring a broadband communication device by downloading configuration information from a central server over a dial-up communications link. However, Baltes neither teaches nor suggests that once the configuration information is downloaded, subsequent access to this information is blocked so that an unauthorized user cannot gain access and download the information.

The Office Action states at page 5, lines 9-12 that:

> Baltes teaches the method of Claim 1, where the access to the database for downloading the file is inherently blocked after the file has been downloaded. **The Examiner interprets blocking access to the database as terminating the link between the database and the router.** (Emphasis added.)

The Applicants respectfully disagree with the Examiner's interpretation of claim 1, which is contrary to the language in claim 1 and the disclosure in the specification. Claim 1 states in relevant part that the method includes:

> permitting access to the database by the user for downloading the file for a period of time;
>
> downloading the file from the database to the managed device; and
>
> blocking access to the database for downloading the file.

Claim 1 clearly teaches that once the file has been downloaded from the database, "access to the database for downloading the file" is blocked. Baltes neither teaches nor suggests that access to the database for downloading the file is blocked under any circumstances.

The specification of the present application explains that the database is only available for downloading the file for a brief window of time or until the file has been downloaded. Thereafter, access to the file is blocked. The specification states at page 7, line 9 to page 8, line 2 that:

> Security is all about risk management and providing systems which minimize a computer network's exposure to risk. The present invention increases security, without the need to use any encryption mechanisms or devices that are hard to maintain, by reducing the time that the configuration file is available for downloading on the Internet. When a service provider makes configuration file (a file that contains configuration information for a particular program -- when the program is executed, it consults the configuration file to see what parameters are

> in effect) or other files available for downloading by a customer over the Internet, the file can be accessed by anyone who has the password and/or access code. This leaves an open door into the service provider's database and allows unauthorized hackers to downloading sensitive files. The method of the present invention opens the door only after the customer has signaled that it is ready to download the files and closes the door immediately after the downloading has been successfully, or in one embodiment unsuccessfully, completed. This allows hackers only a brief opportunity to gain unauthorized access to files in the service provider's database.

The Office Action states that: "The Examiner interprets blocking access to the database as terminating the link between the database and the router." In a very broad sense, this is correct, but it misinterprets claim 1. A dial-up communication link for accessing a database is substantially the same as communicating with a party over the telephone. If the telephone communication link is terminated (either by one partying hanging up or an equipment malfunction), access between two parties ends and communication is at least temporarily blocked. However, in most case, this does not prevent either party from dialing the other party's phone number, reestablishing the telephone communication link and continuing the conversation. Accordingly, the Examiner's interpretation of blocking access to the database as being equivalent to terminating the link does not address the fact that access to the database can be just as easily "unblocked" by reestablishing "the link between the database and the router." Baltes does not address this issue.

In the method disclosed by Baltes, configuration information is downloaded over a dial-up communication link and, when downloading is completed, the dial-up communication link is presumably terminated (Baltes does not disclose terminating the communication link and the

consequences of such an action) and once terminated, access to the database is blocked. However, Baltes does not disclose what would happen if the dial-up communication link was interrupted before the entire configuration file was downloaded. Baltes does not teach that the user would be prevented from reestablishing the dial-up communication link and downloading the configuration file for a second time. Moreover, there is no teaching nor suggestion in Baltes that a hacker having the necessary information could not establish a dial-up communication link between the database and another router from a different location and illegally download the configuration file after the authorized user had already downloaded it.

Baltes teaches that the user is identified using caller ID. However, this would not prevent a hacker from providing a false caller ID and accessing the database. An internet publication from the Commercial Law League of America (a copy is attached as Exhibit A) reports the first case brought by the FTC against a company for transmitting false caller ID data. Moreover, the internet website for the Attorney General of Michigan (a copy is attached as Exhibit B--see page 2) reports that technology is available that allows thieves to choose the information they want to appear on caller ID. Therefore, the identification of the customer disclosed by Baltes (either using caller ID, Smartcard or serial number) can be easily circumvented and, absent any teachings by Baltes to the contrary, a hacker could establish a dial-up communication link with the database and download a configuration file an unlimited number of times without any restrictions.

Accordingly, Baltes does not teach nor suggest "blocking access to the database for downloading the file" as required by claim 1 and the Applicants respectfully request that the Examiner withdraw the rejection of claims 1-4 and 14 as anticipated by Baltes.

Claim Rejections -- 35 USC § 103

Claims 6-8 and 15 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Baltes in view of U.S. Patent No. 6,934,735 to Emens et al. ("Emens"), which discloses a method for controlling the timing of delayed downloads from a server computer to a user or client computer. The user specifies a window of time during which the download needs to be completed and the method uses mathematical formulas to: (1) determine the download time (col. 6, lines 3-10); (2) determine the weighted sum of the ping response time (col. 7, lines 13-20); and (3) set the download time within the specified time interval (col. 6, lines 3-9). The method taught by Emens permits the client computer to download a file at a time of its choosing, not at a time chosen by the server computer. Thus, Emens teaches that the "download scheduling intelligent agent 204" can be implemented as a browser plug-in (see col. 3, lines 30-31) in the client (i.e., user) computer (see col. 3, lines 40-50 and FIG. 2). There is no time limit set by the server computer that restricts the downloading of files by the client computer. Thus, if the user doesn't have an imminent deadline and the resources of the user/client computer are heavily loaded, the files on the server computer can be accessible for days, weeks or even months.

Emens neither teaches nor suggests minimizing the time period during which a file can be downloaded in order to increase the security of the downloaded files and to prevent unauthorized

downloading, nor does Emens teach or suggest that a file can only be downloaded once and that access to the file is blocked after it is downloaded.

The method disclosed by Emens requires the user to specify a window of time and for the user/client computer to determine when to download files. The server computer is not responsible for scheduling downloads. In contrast, in claim 1 of the present invention, the server which stores the file that is to be downloaded restricts the user's access to the database to a period of time. By setting a time period, the server limits access to the database and reduces the opportunity for hackers to gain unauthorized access to the database. Emens does not teach nor suggest such security protection for the database by restricting the time period when the database can be accessed. The database in Emens allows unrestricted access by the user, at the user's convenience. The only time restriction for completing the download is arbitrarily set by the user based on the load on the user computer resources and the network traffic.

The Office Action, at page 7, lines 1-2, cites the Abstract of Emens which states, "a system for accepting a specification of time interval during which a download is to be performed." This statement is confusing because the system that accepts the specification of time is the **user's computer** and the person who selects the specification is the **user**. (See claim 1, "the method on the client computer comprising...") Thus, there is no coordination between the user and the server that is downloading the file. The user unilaterally sets a time interval and there is no coordination with the server. The server provides unrestricted access without any time limitations and the user is left to choose when the user computer will access the server

computer to download files. Thus, the "time interval" in Emens does not provide any security, nor does it prevent a hacker from gaining access to the server and selecting his own time interval. Moreover, Emens does not teach that access to a file is blocked after it has been downloaded as required by the Applicants' claims.

Baltes and Emens do not render claims 6-8 and 15 (nor any of the other claims) obvious, since these references, either alone or together, do not teach or suggest a server for downloading a file which restricts access to the database to a period of time and which blocks access to a file after it has been downloaded. The time interval taught by Emens does not restrict access to the server for downloading. It is only used by the user computer for scheduling a download. Moreover, one of ordinary skill in the art would not find it obvious in view of Emens to set a time interval in the server for downloading files since this would frustrate the purpose of the method taught by Emens. The method taught by Emens could not optimize the resources of the user computer if forced to download files within an arbitrary time window set by the server computer.

Accordingly, the Applicants submit that claims 6-8 and 15 are not obvious in view of Baltes and Emens and respectfully request that the Examiner withdraw the rejection based on these references.

Claims 5, 9-13, 16-17 and 21-24 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Baltes in view of U.S. Publication No. US 2002/0179709 to Mehler ("Mehler"), which discloses a bar code and scanner, but does not disclose a time interval for

accessing the database in the server or blocking access to the database for downloading a file after the file has been downloaded. The teachings in Mehler do not overcome the deficiencies in Baltes. The combination of Baltes and Mehler neither teaches nor suggests a method for setting a time interval for downloading files and then blocking access to the database containing the files either after the file is downloaded or after the expiration of the time interval.

Claims 18-20 and 25 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Baltes in view of Emens as applied to claim 16 above and further in view of Emens. The Applicants respectfully disagree with the Examiner's finding that "[a]ll the limitations of Claim[s] 18-20 and 25 are anticipated in the rejection of claim 16, except that the period of time is predetermined." Office Action, page 10, lines 12-13. Moreover, as discussed in detail above, the disclosure in Emens that "a system for accepting a specification of time interval during which a download is to be performed" (Abstract) has been misconstrued by the Examiner. Emens teaches a method wherein the user computer sets a time interval that is used by a program in the user computer to manage the downloading of files from a server. The time interval taught by Emens is not transmitted to the server and it does not restrict access to the server. Instead, the time interval taught by Emens is used as a mathematical boundary so that formulas can be used to determine the optimum time for downloading files to the user computer. The claims in the present application restrict access to the database to a period of time and require coordination between the server and the user device. Emens neither teaches nor suggests such coordination since the time interval in Emens is unilaterally and arbitrarily selected by the user. As such, the

time interval in Emens neither teaches nor suggests the time interval in the claims of the present application.

The Office Action states at page 10, lines 18-20 that:

> The motivation to combine is "to overcome the problem of long download times" (Emens Column 2, lines 9-11). The motivation for the time period to be less than 1 hours (sic) is to acclimate user's requirement.

The Applicants respectfully disagree with this finding. Emens teaches a method for scheduling downloads to a user computer that is concurrently performing other tasks so that the download occurs when the maximum user computer resources are available. Emens does not schedule downloads based on the computer resources of the server--only the user computer. By scheduling downloads when the user computer is not busy, download times are decreased.

In contrast to Emens, Baltes teaches "a method in which a central server may be contacted when configuration information is needed to install a broadband communication device." Page 1, col. 2, lines 1-3. Thus, the download taught by Baltes occurs when a device is being installed and at a time when the device is not performing any other functions which would consume computer resources. The files downloaded to the devices taught by Baltes do not experience long download times because they are not performing other tasks that use up computer resources. When configuration files are downloaded using the method taught by Baltes, the downloading is the sole function of the user device (i.e., the user computer). Therefore, the user computers/devices in Baltes do not experience a "problem of long download

times" and, even if they did, Emens' method of scheduling downloads based on the availability of resources in the user computer would not solve the problem because the user computer taught by Baltes is not performing other tasks or functions. Accordingly, one of ordinary skill in the art would not combine the teachings of Baltes and Emens because Emens teaches a method for scheduling downloads to a user computer that is expending resources performing other tasks, while Baltes teaches a method for downloading to a user computer that is not performing other tasks and always has the maximum computer resources available.

Finally, the Office Action states at page 11, line 1 that; "It is inherent that downloading will be blocked if there is a time limit for downloading." As explained above, the method for scheduling downloads taught by Emens is performed in the user computer (see claim 1, "the method in the client computer comprising") and the time limit for downloading the files is set by the user. There is no teaching nor suggestion by Emens that the time limit is transmitted to the server or that the server responds in any way to the time limit. Thus, the time limit applies only to the user computer and, if the downloading is blocked, it is blocked at the user computer and not at the server.

The claims of the present invention refer to "blocking access to the database for downloading the file" (see claim 1) and the method is intended to prevent unauthorized users from accessing the database and downloading the files. If the time interval disclosed in Emens uses a time limit to block the user computer from receiving downloads, it still leaves the server vulnerable to hackers and it does not prevent the downloading of the files by a hacker.

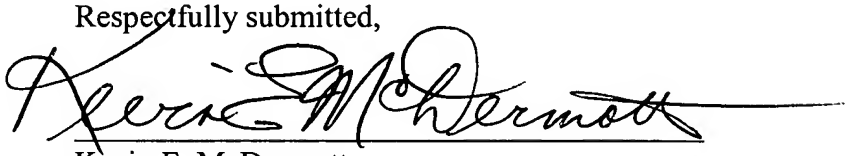
Therefore, the time intervals in Emens and in claim 1 of the present application are clearly distinguishable and one of ordinary skill in the art would not find that Emens teaches blocking access to the server database after the expiration of a time interval.

Conclusion

The Applicants submit that the arguments set forth above clearly distinguish the prior art references cited in the Office Action from the pending claims and, therefore, respectfully request early allowance of the claims.

If the Examiner has any questions or comments relating to the present application, he or she is respectfully invited to contact Applicants' attorney at the telephone number set forth below.

Respectfully submitted,



Kevin E. McDermott
Registration No.: 35,946
Attorney for Applicants

HOFFMANN & BARON, LLP
6900 Jericho Turnpike
Syosset, New York 11791
(516) 822-3550
KEM:dlb
232376_1

COMMERCIAL LAW LEAGUE OF AMER
LEADING THE WAY

Washington Hot News

2004 Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
2005 Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
2006 Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
2007 Jan

FTC Initiates First Case of False Caller ID Data

May 17, 2006
Scorpio Systems, Ltd., a financial product marketer, is the first organization subject to federal accusations of transmitting false caller ID information (the government alleges Scorpio did not transmit a caller ID or sent a phony caller ID), according to an April 26 complaint filed by the Justice Department in the U.S. District Court for the District of New Jersey (U.S. v. Venkataraman, D. N.J., 4/26/06).

David Goch

Washington Legislative Counsel
Commercial Law League of America
dgoch@wc-b.com

Washington Hot News for May, 2006

House Commerce Committee Elected to

Telemarketing Fraud - Never Give Personal Information to Unknown Callers Updated 10/2006

CONSUMER ALERT

MIKE COX
ATTORNEY GENERAL

The Attorney General provides Consumer Alerts to inform the public of unfair, misleading, or deceptive business practices, and to provide information and guidance on other issues of concern.

Telemarketing Fraud
Never Give Personal Information to Unknown Callers

TELEMARKETING FRAUD LIMITED ONLY BY CRIMINAL'S IMAGINATION

The stories change over time but the purpose and result of the call to the victim remains the same. The thief gains the victim's confidence and the victim divulges personal information. Victims are ashamed they fell for the bait and often do not report the crime to law enforcement, family, or even friends. Meanwhile, the thief uses the personal information to drain the victim's bank account, obtain credit in the victim's name, or commit some other crime.

Thieves frequently relay a sense of urgency, pretending to be bank or credit card officials, government employees, law enforcement, or other trusted professionals to fool victims into providing information. A few of the recent schemes used to lure information from victims include a story that the personal information is necessary for any of the following reasons:

- to protect the call recipient from becoming the victim of fraud;
- to claim a shopping spree or valuable gasoline coupons in return for a minimal processing charge to be debited directly from your bank account;
- to qualify for a new government program or to continue in a current government program like Medicare or Social Security;
- to claim a prize or to be eligible for a pre-approved credit card, loan, or government grant;
- to dispute the victim's failure to report for jury duty, the consequence of which is being arrested;
- to qualify for discount programs; or
- for a program or charity tied to recent news events or tragedies;

There are even reports that criminals have become so bold that they

Related Conte
- Fraudulent E-r Intend to Steal Personal Infor Updated 11/2C
- 'Tis The Seasc Protecting You Making Purcha
- Identity Theft I for Michigan C 2006 Update 1
- Long-Term Re Programs 10/2
- Pharming - Ye Tool Used By I Thieves 9/200
- A Job Offer To Be True 9/200
- Your Social Se Number 9/200
- Advance-Fee I 7/2006
- Annuities - Are Right Investme 5/2006
- Increased Gas Again? 4/2006
- Internet Safety 4/2006
- Talent Scoutin 4/2006
- Are You Payin For Your Pres Drugs? Shop A Find Out! 2/20
- Free Annual C Reports-What Should Know-- 2/2006
- Home Lending Foreclosure R 1/2006
- Item Pricing (S Frequently Ask 1/2006
- Used Vehicle I For Flood Dam
- Sony Music CI Identity Theft F Worldwide Exc Program 11/2C
- Business Opp 11/2005
- Lead and Chil

call and report personal information is necessary because of a recent family tragedy. For instance, money is needed to rush a family member to emergency medical care or your personal information is necessary before you can get more information about a family member in crisis.

The Attorney General warns that in the face of negative publicity the scam artists often change the name of the company involved and modify the pitch, but the purpose -- to steal personal information -- remains constant.

NEVER GIVE PERSONAL INFORMATION TO SOMEONE WHO CALLS

Con artists will lie, cheat, steal, and make up plausible stories to convince you to divulge sensitive information. The callers are often professional criminals who are skillfully able to get personal information before the victim has time to properly assess the situation.

The information requested may seem minimal -- for instance just the numbers off the bottom of your check. Armed with these numbers, however, thieves can drain your bank account. Your Social Security number will allow a crook to obtain credit and charge thousands of dollars to your good name. Even information as simple as your maiden name or birthday can be used to rob you.

THIEVES CHOOSE NUMBER THEY WANT TO APPEAR ON CALLER ID

Technology available for purchase on the Internet allows crooks to use a fake caller ID to make bogus phone calls look like they are coming from a legitimate and trustworthy source to gain access to a victim's valuable personal information.

False caller ID numbers have been reported in connection with fraudulent calls claiming the potential victim missed jury duty and to avoid arrest or a fine must "verify" their Social Security number or other personal information. The calls may seem legitimate because the telephone number of the local courthouse shows up on the caller ID.

DEMAND DRAFTS -- WHY PROVIDING BANK INFORMATION IS A PROBLEM

When providing checking account numbers and bank routing numbers (numbers reproduced at the bottom of the check) over the phone, you are giving the caller the opportunity to withdraw money from your account as if you had written a check. In most states, including Michigan, you can pre-authorize a draft from your checking account. This occurs when you provide your checking account and bank routing numbers and authorize a certain amount of money to be withdrawn from your account. Your signature is not required for money to be drawn out of a checking account in this manner. Demand drafts closely resemble checks and are processed through the check clearing system, which handles millions of items daily.

Once you provide your account information to another person, you cannot control how that person uses the information. Accounts may easily be accessed by unauthorized demand drafts or for larger amounts than authorized.

IF YOU HEAR A STORY YOU BELIEVE . . .

If you receive a call that convinces you divulging personal information is necessary, **STOP**! If you feel you must divulge information, take the following steps:

1) Confirm the identity of the caller (your bank, credit card company, governmental agency, police department, etc. . .);

2) Hang up!;

3) Go to a reliable source for the phone number of the caller (a statement, a bill, or your phone book – **do not rely on the number the caller provides**);

4) Call the identified source to confirm whether the prior call you received was legitimate;

5) If it was not legitimate, report the attempted fraud to the Attorney General's office so we can investigate and update our consumer warnings.

TRADITIONAL WARNING SIGNS

A caller may tell you:

- You've won a "free" gift, vacation, or prize. But you have to pay for "postage and handling," "taxes," "insurance," or other charges. If a caller tells you the payment is for taxes, he or she is violating federal law.
- You must act "now" or the offer will expire.
- You must mail or wire transfer money, give a credit card or bank account number, or have a check picked up by courier.
- You don't need to check out our company, the offer is "guaranteed" and "risk-free."
- You can't afford to miss this "high-profit, no-risk" offer.

If you hear these (or similar) pitches just say "NO" and hang up the phone.

ADDITIONAL TIPS TO AVOID TELEMARKETING FRAUD

It's very difficult to get your money back if you've been cheated over the phone. Before you buy anything by telephone, remember:

- Don't buy from an unfamiliar company. Legitimate businesses understand that you want more information about their company and are happy to comply.
- Always ask for, and wait until you receive, written material about

any offer or charity. If you get brochures about costly investments, ask someone whose financial advice you trust to review them. But, unfortunately, you still must be cautious as not everything written down is true.

- If you insist on purchasing over the phone, obtain a salesperson's name, business identity, telephone number, street address, mailing address, and business license number before you transact business. Some con artists give out false names, telephone numbers, addresses, and business license numbers. Verify the accuracy of these items and use a credit card so you can dispute the charge if necessary.

- Before you give money to a charity or make an investment, find out what percentage of the money is paid in commissions and what percentage actually goes to the charity or investment.

- Before you send money, ask yourself a simple question, "What guarantee do I really have that this solicitor will use my money in the manner we agreed upon?"

- Do not pay in advance for services. Pay for services only after they are delivered.

- Some criminals will send a messenger to your home to pick up money, claiming it is part of their service to you. In reality, they are taking your money without leaving any trace of who they are or where they can be reached.

- Always take your time making a decision. Legitimate companies won't pressure you to make a snap decision.

- It's never rude to wait and think about an offer. Be sure to talk over big investments offered by telephone salespeople with a trusted friend, family member, or financial advisor.

WHAT TO DO IF YOU FALL VICTIM

Bank Account Information

If you mistakenly provide bank account information to a suspicious caller, take the following steps immediately:

- Call your bank, explain the circumstances, and tell them you want to take all necessary steps to block unauthorized withdrawals. Follow up your call with a visit to the bank and written notification. Keep a copy of the written notification. Your bank will likely charge you a fee for stopping the payment.

- If the money has already been withdrawn, immediately ask the bank to credit your account because the debit was not authorized. To get this credit, you may need to submit a sworn statement to your bank that the debit was unauthorized. This statement is called a "Written Statement Under Penalty of Perjury," and you may get a copy from your bank.

As a precaution, always check your bank statements to make sure that there are no unauthorized payments. Report any unauthorized

payments to the bank as soon as you detect them. In the case of unauthorized demand drafts, you may also wish to close the account to avoid any further unauthorized withdrawals by persons who have gained access to your account information. Be aware that con artists may sell your information to other bad actors.

Other Personal Information
If the information you provided is specific to an account, immediately call the security or fraud department of that company. Follow up in writing by certified mail return receipt requested and include copies (not originals) of supporting documents. You may wish to close the relevant account.

In addition, anytime you mistakenly provide personal information to somebody who calls, you should immediately place an initial fraud alert on your credit report for at least 90 days. When you place an initial fraud alert on your credit report, you are entitled to one free credit report from each of the three nationwide consumer reporting companies.

You can place the initial fraud alert by contacting the toll-free fraud number of any of the three consumer reporting companies below. You only need to contact one of the three companies to place an alert. The company you call is required to contact the other two, which will place an alert on their versions of your report too.

Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241

Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013

TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Once you get your free credit report, review it carefully. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain. Check that personal information, like your Social Security number, address(es), name or initials, and employers are correct. If you find fraudulent or inaccurate information, get it removed. See the "Correcting Credit Reports" section of the Federal Trade Commission's booklet, "Take Charge: Fighting Back Against Identity Theft" available at www.ftc.gov/idtheft or by calling toll free 1-877-ID-THEFT (877-438-4338); TTY: 866-653-4261.

FREE ANNUAL CREDIT REPORTS

For more information on your right to obtain annually one free credit report from each credit reporting agency, regardless of circumstances, see the Attorney General's alert "Free Annual Credit Reports – What Consumers Should Know" available on the Attorney General's Web site or by using the contact information provided below. Free annual reports are available by calling toll free 1-877-322-8228.

REDUCE TELEMARKETING CALLS

To reduce telemarketing calls, consumers should put their phone number on the Federal Trade Commission's Do Not Call Registry. Register by phone toll free (1-888-382-1222; TTY 1-866-290-4236

from the phone number you want to put on the registry) or online at www.donotcall.gov.

REPORT TELEMARKETING FRAUD

Contact the Attorney General's Consumer Protection Division at:

Consumer Protection Division
P.O. Box 30213
Lansing, MI 48909
517-373-1140
Fax: 517-241-3771
Toll free: 1-877-765-8388
www.michigan.gov/ag (online complaint form)